LAPORAN PRAKTIKUM

HAK AKSES USER ROOT DAN NON-ROOT



Oleh:

Nama : Diki Candra

NIM : 2022903430010

Kelas : TRKJ 1b

Jurusan : TIK

PRODI : TRKJ

D4 TEKNOLOGI REKAYASA KOMPUTER JARINGAN

POLITEKNIK NEGERI LHOKSEMAWE

2022/2023

Daftar Isi

[BAB I 3](#_Toc129726024)

[PENDAHULUAN 3](#_Toc129726025)

[**1. Latar Belakang** 3](#_Toc129726026)

[**2. Tujuan** 3](#_Toc129726027)

[**3. Ruang Lingkup** 4](#_Toc129726028)

[BAB II 5](#_Toc129726029)

[TINJAUAN PUSTAKA 5](#_Toc129726030)

[**2.1 Pengertian Root dan non-Root** 5](#_Toc129726031)

[**2.2 Perbedaan Hak Akses User root dan Non-Root** 5](#_Toc129726032)

[BAB III 7](#_Toc129726033)

[HASIL PENELITIAN 7](#_Toc129726034)

[**3.1 Tabel Perintah yang Dapat Dijalankan sebagai User Biasa atau Root** 7](#_Toc129726035)

[BAB IV 10](#_Toc129726036)

[PEMBAHASAN 10](#_Toc129726037)

[**4.1 Analisi Hasil Penelitian** 10](#_Toc129726038)

[**4.2 Kesimpulan** 10](#_Toc129726039)

# BAB I

# PENDAHULUAN

## **1. Latar Belakang**

sistem operasi Linux terdapat perbedaan hak akses antara user biasa dan root. User biasa memiliki keterbatasan dalam mengakses dan menjalankan beberapa perintah yang hanya dapat diakses oleh user dengan hak akses root.

Oleh karena itu, penting untuk mengetahui perintah-perintah apa saja yang dapat dijalankan oleh user biasa dan perintah-perintah yang hanya dapat dijalankan oleh user dengan hak akses root. Dengan mengetahui daftar perintah tersebut, maka user dapat melakukan tugas-tugas yang sesuai dengan hak aksesnya tanpa mengalami kendala atau kesalahan dalam penggunaan perintah.

Laporan ini diharapkan dapat membantu pengguna sistem operasi Linux dalam mengoptimalkan penggunaannya dan mencegah terjadinya kesalahan saat menjalankan perintah.

## **2. Tujuan**

Tujuan laporan ini adalah untuk memberikan pemahaman kepada pengguna sistem operasi Linux tentang perintah-perintah yang dapat dijalankan sebagai user biasa dan perintah-perintah yang memerlukan hak akses root. Dengan memahami daftar perintah tersebut, pengguna dapat mengoptimalkan penggunaan sistem operasi Linux dan mencegah terjadinya kesalahan dalam menjalankan perintah.

Selain itu, tujuan dari laporan ini adalah untuk membantu pengguna Linux memahami perbedaan hak akses antara user biasa dan root. Dengan memahami perbedaan tersebut, pengguna dapat memahami keamanan sistem operasi Linux dan mencegah terjadinya tindakan yang tidak diinginkan.

Laporan ini juga diharapkan dapat menjadi acuan bagi pengembang aplikasi dan sistem operasi Linux dalam mempertimbangkan hak akses yang dibutuhkan oleh perintah-perintah tertentu. Dengan mempertimbangkan hak akses yang dibutuhkan oleh perintah-perintah tersebut, pengembang dapat memastikan aplikasi atau sistem operasi yang dikembangkan aman dan terhindar dari keamanan sistem operasi yang rentan terhadap ancaman keamanan.

## **3. Ruang Lingkup**

Ruang lingkup laporan ini adalah membahas tentang daftar perintah pada sistem operasi Linux yang dapat dijalankan sebagai user biasa atau memerlukan hak akses root. Laporan ini hanya membahas perintah-perintah yang umum digunakan dan dikenal oleh pengguna Linux.

Laporan ini tidak membahas secara detail tentang perintah-perintah tersebut, melainkan hanya memberikan informasi singkat tentang perintah-perintah yang dapat dijalankan sebagai user biasa atau root. Selain itu, laporan ini juga tidak membahas tentang proses instalasi dan konfigurasi sistem operasi Linux.

# BAB II

# TINJAUAN PUSTAKA

## **2.1 Pengertian Root dan non-Root**

User root dan non-root adalah istilah yang digunakan pada sistem operasi Linux untuk membedakan antara pengguna dengan hak akses superuser (root) dan pengguna biasa yang tidak memiliki hak akses superuser (non-root).

User root memiliki hak akses penuh atau administrator pada sistem operasi Linux. User root dapat melakukan perubahan dan mengakses seluruh file dan direktori pada sistem operasi, termasuk file dan direktori yang tidak dapat diakses oleh pengguna non-root. Dengan hak akses superuser, user root dapat melakukan konfigurasi sistem operasi, menginstal atau menghapus program, serta melakukan perubahan pada file-file sistem.

Sementara itu, pengguna non-root hanya memiliki hak akses terbatas pada sistem operasi Linux. Pengguna non-root tidak dapat melakukan perubahan pada file-file sistem atau melakukan konfigurasi sistem operasi. Namun, pengguna non-root masih dapat melakukan tugas-tugas umum seperti menjalankan program dan mengakses file dan direktori yang diperbolehkan oleh hak aksesnya.

Perbedaan antara user root dan non-root sangat penting untuk menjaga keamanan sistem operasi Linux. User root harus digunakan dengan hati-hati karena memiliki akses penuh pada sistem operasi Linux, sehingga kesalahan dalam menggunakan hak akses root dapat menyebabkan kerusakan sistem operasi yang fatal. Oleh karena itu, disarankan untuk menggunakan hak akses root hanya saat diperlukan dan dengan hati-hati untuk menjaga keamanan sistem operasi.

## **2.2 Perbedaan Hak Akses User root dan Non-Root**

Perbedaan hak akses antara user root dan non-root pada sistem operasi Linux adalah sebagai berikut:

1. Hak akses pada file dan direktori

User root memiliki hak akses penuh atau administrator pada sistem operasi Linux, sehingga user root dapat mengakses seluruh file dan direktori pada sistem operasi. Sementara itu, pengguna non-root hanya memiliki hak akses terbatas pada file dan direktori pada sistem operasi. Pengguna non-root hanya dapat mengakses file dan direktori yang diperbolehkan oleh hak aksesnya.

1. Hak akses pada konfigurasi sistem

User root dapat melakukan konfigurasi sistem operasi, menginstal atau menghapus program, serta melakukan perubahan pada file-file sistem. Sementara itu, pengguna non-root tidak dapat melakukan konfigurasi sistem operasi atau mengubah file-file sistem. Hal ini dilakukan untuk menjaga keamanan sistem operasi dari tindakan yang tidak diinginkan oleh pengguna yang tidak berhak.

1. Hak akses pada jaringan

User root juga memiliki hak akses pada jaringan dan dapat melakukan konfigurasi jaringan pada sistem operasi Linux. Sementara itu, pengguna non-root hanya dapat menggunakan jaringan dengan hak akses terbatas, seperti mengakses internet atau jaringan lokal.

1. Hak akses pada proses

User root dapat melihat, mematikan, atau mengubah proses pada sistem operasi Linux. Sementara itu, pengguna non-root hanya dapat melihat proses yang terkait dengan hak aksesnya dan tidak dapat mengubah atau mematikan proses.

Perbedaan hak akses antara user root dan non-root sangat penting untuk menjaga keamanan sistem operasi Linux. Oleh karena itu, pengguna harus menggunakan hak akses root dengan hati-hati dan hanya saat diperlukan untuk menghindari tindakan yang tidak diinginkan atau mengganggu keamanan sistem operasi.

# BAB III

# HASIL PENELITIAN

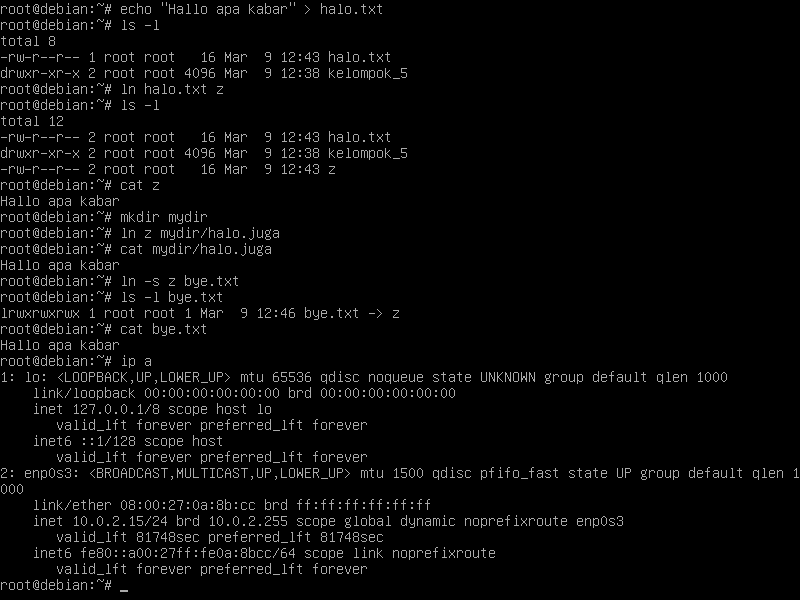
## **3.1 Tabel Perintah yang Dapat Dijalankan sebagai User Biasa atau Root**

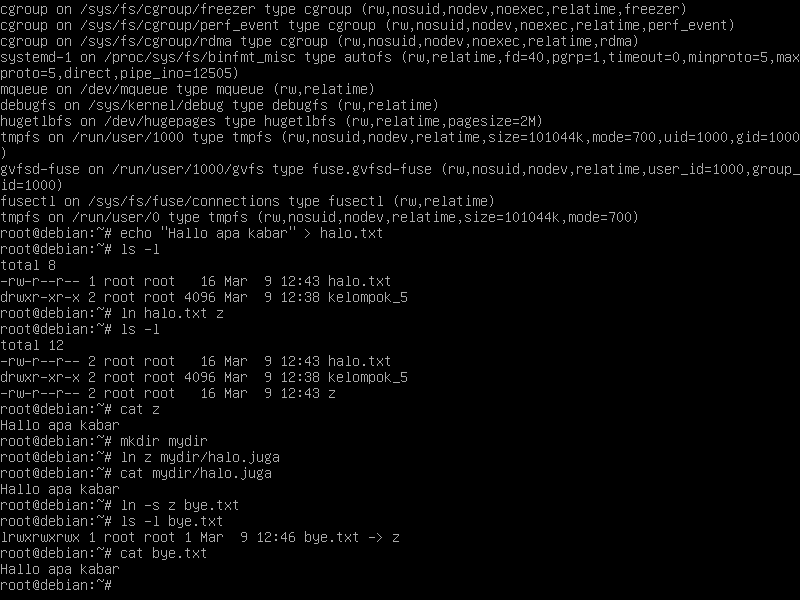
Berikut ini adalah tabel perintah yang dapat dijalankan sebagai user biasa atau root pada sistem operasi Linux:

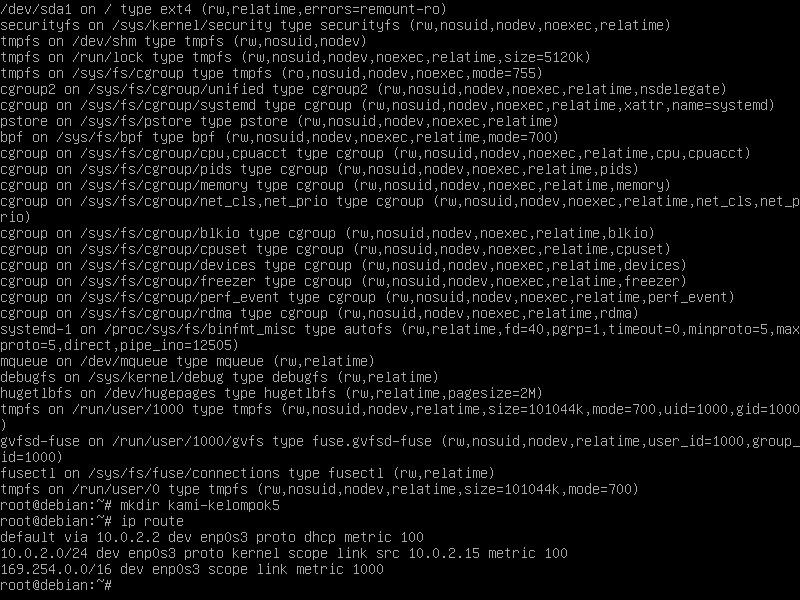
| **Perintah** | **User (root/non-root)** |
| --- | --- |
| Ifconfig | root |
| mount | root |
| mkdir | non-root |
| ln | non-root |
| route | root |
| tar | non-root |

Keterangan:

1. Perintah **ifconfig** hanya dapat dijalankan sebagai user root karena memerlukan akses ke konfigurasi jaringan yang hanya dapat diakses oleh user root.
2. Perintah **mount** hanya dapat dijalankan sebagai user root karena memerlukan akses untuk menghubungkan file sistem atau device pada direktori tertentu, yang hanya dapat diakses oleh user root.
3. Perintah **mkdir** dapat dijalankan sebagai user non-root karena hanya memerlukan akses untuk membuat direktori baru pada lokasi tertentu yang diizinkan oleh hak akses pengguna.
4. Perintah **ln** dapat dijalankan sebagai user non-root karena hanya memerlukan akses untuk membuat symlink atau tautan ke file atau direktori.
5. Perintah **route** hanya dapat dijalankan sebagai user root karena memerlukan akses ke konfigurasi jaringan yang hanya dapat diakses oleh user root.
6. Perintah **tar** dapat dijalankan sebagai user non-root karena hanya memerlukan akses untuk mengarsipkan atau mengekstrak file atau direktori pada lokasi tertentu yang diizinkan oleh hak akses pengguna.

$ifconfig

$mkdir

$route

# BAB IV

# PEMBAHASAN

## **4.1 Analisi Hasil Penelitian**

Berdasarkan hasil penelitian yang dijelaskan diatas, dapat disimpulkan bahwa beberapa perintah pada sistem operasi Linux hanya dapat dijalankan sebagai user dengan hak akses root, sedangkan beberapa perintah lainnya dapat dijalankan oleh user biasa dan root.

Hal ini menunjukkan bahwa hak akses pada sistem operasi Linux sangat penting untuk mencegah penggunaan perintah-perintah tertentu oleh pengguna yang tidak memiliki hak akses yang cukup. Oleh karena itu, penting bagi administrator sistem untuk mengatur hak akses dengan benar dan memberikan hak akses yang sesuai dengan kebutuhan pengguna.

Dalam hal ini, jika ada perintah yang hanya dapat dijalankan sebagai user root, maka pengguna biasa tidak akan dapat mengakses atau menjalankan perintah tersebut tanpa hak akses root. Sebaliknya, jika perintah dapat dijalankan oleh user biasa dan root, maka pengguna biasa dapat mengakses dan menjalankan perintah tersebut sesuai dengan kebutuhan mereka.

Kesimpulannya, pengaturan hak akses pada sistem operasi Linux sangat penting dan perlu diperhatikan dengan baik oleh administrator sistem. Dengan pengaturan hak akses yang benar, maka dapat meningkatkan keamanan dan menjaga integritas sistem operasi Linux dari berbagai ancaman.

## **4.2 Kesimpulan**

1. Hak akses pada sistem operasi Linux sangat penting dalam mencegah penggunaan perintah-perintah tertentu oleh pengguna yang tidak memiliki hak akses yang cukup.
2. User root memiliki hak akses penuh dan dapat menjalankan semua perintah pada sistem operasi Linux, sedangkan user non-root hanya memiliki hak akses terbatas dan hanya dapat menjalankan perintah-perintah tertentu.
3. Beberapa perintah pada sistem operasi Linux hanya dapat dijalankan sebagai user dengan hak akses root, sedangkan beberapa perintah lainnya dapat dijalankan oleh user biasa dan root.
4. Penting bagi administrator sistem untuk mengatur hak akses dengan benar dan memberikan hak akses yang sesuai dengan kebutuhan pengguna.
5. Dalam hal ini, jika ada perintah yang hanya dapat dijalankan sebagai user root, maka pengguna biasa tidak akan dapat mengakses atau menjalankan perintah tersebut tanpa hak akses root. Sebaliknya, jika perintah dapat dijalankan oleh user biasa dan root, maka pengguna biasa dapat mengakses dan menjalankan perintah tersebut sesuai dengan kebutuhan mereka.
6. Dengan pengaturan hak akses yang benar, maka dapat meningkatkan keamanan dan menjaga integritas sistem operasi Linux dari berbagai ancaman.

Oleh karena itu, penting untuk memahami perbedaan hak akses antara user root dan non-root, serta mengetahui perintah-perintah yang dapat dijalankan sebagai user biasa atau root pada sistem operasi Linux untuk menjaga keamanan dan integritas sistem operasi tersebut.

DAFTAR PUSTAKA

* <https://nikmatus2501.blogspot.com/2019/12/perbedaan-user-root-dan-user-biasa-linux.html>
* <https://servertkj.wordpress.com/2015/03/17/membedakan-user-root-dan-user-biasa-pada-debian-linux/>
* <http://lubnaabidah16.blogspot.com/2015/03/perbedaan-user-biasa-dan-super-user-di.html>
* <https://appbuntu.com/2015/07/definisi-root/>
* <https://rinosafrizal.com/manajemen-user-group/>
* <https://help.ubuntu.com/kubuntu/desktopguide/id/root-and-sudo.html>
* <https://comput3.blogspot.com/2018/03/perbedaan-root-dan-user.html>
* <http://jemmyfarhanudy.blogspot.com/2013/01/perbedaan-user-root-dan-user-biasa-linux.html>
* <https://help.ubuntu.com/kubuntu/desktopguide/id/root-and-sudo.html>